E.F.T und Datenschutz

Poullet, Yves

Published in:
Datenschutz und Datensicherung

Publication date:
1988

Document Version
le PDF de l'éditeur

16 Vgl. Simitis, in: Simitis u.a. (o. Fn. 15), § 45 Rn. 18; Schneider, in: Gallwas-Schneider- Schwappach-Schweinoch-Steinbrinck, DatenschutzR, Stand Januar 1986, §45 Rn. 6.
17 Vgl. OLG Düsseldorf (o. Fn. 8), NJW 1985, 2538.
18 Vgl. VGH Mannheim, NJW 1984, 1911, 1912 Hirte (o. Fn. 4), NJW 1986, 1900; Schimpf, DÖV 1985, 266 m. zahlr. Nachw.
19 Vgl. Ordemann/Schomerus, BDSG, 3. Aufl., 1982, §11 Anm. 1.2; Auernhammer, BDSG, 1977, §11 Rn.8.
20 Dies verkennt Schimpf (o. Fn.4), DÖV 1985, 267.
21 S.o. Fn 14
22 Gola, Handwerksrolle und Datenschutz, RDV 1987, 225f., 227.
23 Fn. 3.
24 NJW 1986, 2330.
25 BVerfG (o. Fn. 7).
26 BVerfGE 65,44 = NJW 1984,422 (o. Fn.7).
27 Vgl. OLG Düsseldorf (o. Fn.8), NJW 1985, 2538.
28 Vgl. allg. BVerfGE 64, 229(242); speziell im Zusammenhang mit „berechtigtem Interesse" Simitis, Die informationelle Selbstbestimmung – Grundbedingungen einer verfassungskonformen Informationsordnung, NJW 1984,398f., 401.
29 NJW 1985, 2538.
30 Vgl. Schimpf (o. Fn. 4), DÖV 1985, 268.
31 Hirte (o. Fn. 4), NJW 1986, 1902.
32 So Schimpf, DÖV 1985, 269 unter Berufung auf das „Prinzip der Veräußerlichung".
33 Hirte, NJW 1986, 1901.
34 So aber offenbar Hirte, NJW 1986, 1901, 1902.
35 Vgl. Schneider, in: Gallwas u.a. (o. Fn.16), §45 Rn. 11.
36 Vgl. LG Berlin (o. Fn. 2), das nur bei einem mittels EDV geführten Register die Belange des Betroffenen (= Schuldner) berücksichtigen will; vgl. auch den „Entwurf eines Gesetzes zur Änderung von Vorschriften über das Schuldnerverzeichnis" sowie den „Entwurf einer Verordnung über die Erteilung von Abdrucken und Listen aus den Schuldnerverzeichnissen" (Stand: 28.8.1987), die einerseits einen verstärkten Schutz der Persönlichkeitssphäre des Schuldners bezwecken, andererseits die berechtigten Interessen der Wirtschaft am Schutz des redlichen Geschäftsverkehrs berücksichtigen sollen.

E.F.T. und Datenschutz*)

Yves Poullet

Abstrakt: *Bei Barzahlungen fallen keine personenbezogenen Daten an. Bei Teleshopping und Telebanking hingegen werden Daten erfaßt, da mehrere Stellen an den anfallenden Daten interessiert sind. Deshalb ist eine spezialgesetzliche Datenschutzregelung notwendig. Dem kommen Bankgeheimnis und Briefgeheimnis entgegen. Datenschutz auf EFT, Electronic Fund Transfer, und POS, Point of Sale, angewandt; legt nahe, im Sinne der „Speichernden Stelle" des BDSG einen Verantwortlichen für das Netz zu definieren. Das weitere Recht sollte sich an den Grundsätzen von Treu und Glauben, der Sicherheit und der Zweckmäßigkeit orientieren. Dem Betroffenen sollen Informationen und Datenströme transparent gemacht werden. Landesübergreifende, insbesondere europäische Gesichtspunkte, sind zu berücksichtigen.*

Einleitung: Der informative Wert elektronischer Zahlungen

Zu Beginn unserer Erörterung der Probleme, die uns die E.F.T. im Rahmen der persönlichen Freiheiten stellen, obliegt es uns festzustellen, daß der Gebrauch dieser neuen Zahlungsmodi die Natur des Zahlungsaktes verändert (Brown, Godschalk).

Der informative Wert einer Barzahlung ist nahezu gleich null. Die Barzahlung liefert dem Kaufmann keinerlei Informationen über die Identität des Käufers. Somit kann er schwerlich eine Verbindung (Korrelation) zwischen einer bestimmten Person und einer bestimmten Zahlung herstellen. Der Bankier seinerseits, steht ganz und gar außerhalb des Konsumierungsaktes, es sei denn im Außnahmefall des Erwerbs im Rahmen eines durch ihn gewährten Kredites.

Eine Zahlung mittels Scheck erhöht kaum den informativen Wert. Jedoch kennt der Kaufmann nun nicht nur die Identität seines Kunden, sondern auch dessen Verbindung mit einem Finanzinstitut in diesem Falle demjenigen, welches die Scheckformulare ausgeliefert hat. Der Bankier weiß nun von einer geschäftlichen Verbindung zwischen seinem Kunden und einem Handelsunternehmen, jedoch nur unter der Bedingung, daß der Scheck auch den Namen des Kaufmannes trägt. Diese Informationen sind jedoch nur während der Aufbewahrungsdauer des Schecks verfügbar.

Im Falle eines E.F.T. erhält die Zahlung einen ungleich größeren informativen Wert als bei allen anderen Zahlungsmodi. So erlaubt die Abhebung an einem Geldausgabeautomaten (Automatic Teller Machine, A.T.M) dem Bankier sowohl die Identität des Abhebenden als auch Zeitpunkt und Ort der Abhebung zu speichern. Den Bankier informiert die Benutzung eines P.O.S. über die Identität des Kaufmannes, über Ort und Zeitpunkt und selbst über die Natur der Transaktion. Seinerseits verfügt der Kaufmann sofort über Informationen bezüglich der Li-

*) E.F.T. steht für "Electronic Fund Transfer", Transaktion von Geld mittels elektronischer Systeme.
Mitarbeit und Übersetzer: Helmut Havenith

quidität (Zahlungsfähigkeit) seines Kunden, sowie der Existenz eines Kontos bei einem bestimmten Bankinstitut. Die Nutzung der Datenverarbeitung bei der Verwaltung dieser Daten erhöht noch ihren informativen Wert, denn es sind erst die Gruppierung dieser primären Informationen, die Feststellung von Überschneidungen und Vergleiche, die es erlauben, ein genaues Bild (Image) der Verbrauchsgewohnheiten, der Aufenthaltsorte, der Höhe der Ausgaben, usw. einer Person zu erstellen.

Mit anderen Worten, aufgrund ihres direkten und indirekten informativen Wertes entstehen beim Telebanking und Teleshopping gewisse **spezifische** Gefahren zusätzlich zu den im **allgemeinen** bei der Benutzung telematischer Dienstleistungen vorzufindenden.

Das erste Kapitel stellt diese besonderen Gefahren der Telebanking- und Teleshoppingoperationen heraus, die dem gewöhnlichen Verbraucher entstehen. Das zweite Kapitel analysiert und bewertet die gesetzlichen Regelungen, die auf diesen Gebieten angewandt werden.

1 Die besonderen Gefahren bei E.F.T.-Operationen

Der Gebrauch gleichwelcher telematischer Dienstleistung erlaubt es, den Zeitpunkt der Benutzung der Dienstleistung, sowie den Aufenthaltsort zu dieser Zeit (z.B. zu Hause, ...) festzustellen. Die Art der Dienstleistungen beim Telebanking und Teleshopping erwecken noch weitere Befürchtungen. So können nun die Verbrauchsgewohnheiten, die Zusammensetzung des Vermögens und die Art und Weise der Verwaltung desselben, festgestellt werden. Die Standorte der A.T.M. und der P.O.S. erlauben es, die Aufenthaltsorte eines Verbrauchers zu überprüfen.

Wie auch der amerikanische O.T.A. bemerkt:

"With increased use of E.F.T. these will be a large number of points at wich traditional norms of privacy could be invaded. More E.F.T. Terminals will be online, making Electronic Surveillance a more credible possibility. Single Statement reporting of all kinds of financial transactions will become common, more data will be aggregated and thus easier to acces. At the same time, there could be broader and swifter dissemination of inaccurate data. Even if customer correction of data is facilitated, it will be more difficult for corrections to catch up with and replace faulty information".

Um diese besonderen Gefahren zu veranschaulichen, erörtern wir in einem ersten Abschnitt die **Art der Daten,** die dem Telebanking eigen sind. Ein zweiter Abschnitt beschäftigt sich mit **dem Ort ihrer Verarbeitung und Speicherung,** wobei wir jedoch der Verschiedenheit der beteiligten Personen und ihrer jeweiligen Interessen Rechnung tragen.

Schließlich sind es die verarbeiteten Daten und die Verschiedenheit der beteiligten Personen, die die besondere Aufmerksamkeit, die man dem Datenschutz bei der Einrichtung und Verwirklichung von dem Verbraucher zugänglichen telematischen Dienstleistungen widmet, berechtigen (Bing, Poullet).

Die Erörterung dieses Abschnittes erfordert zuvor noch einige allgemeine Bemerkungen.

Zum ersten, handelt es sich um personenbezogene Daten, die durch die Benutzung der Dienstleistung entstehen. Der vertrauliche Charakter dieser Daten entsteht nicht so sehr durch den Inhalt der Datenbank an sich (die meisten der in ihr enthaltenen Informationen sind banaler Art), sondern erst durch die Benutzung der Datenbank durch den Verbraucher. Diese Benutzung bereichert die Datenbank und erlaubt es somit ein typisches Profil eines Verbraucher oder einer Verbrauchergruppe zu erstellen.

Zum zweiten kennzeichnet sich die Benutzung dieser Dienstleistungen durch die Unsicherheit der Datenkanäle, über die die durch die Benutzung entstandenen Informationen übertragen werden.

Dies geht vorwiegend aus zwei Ursachen hervor:

- der Servicer einer Dienstleistung ist nicht notwendigerweise identisch mit der Person, die für ihre technische Realisierung zuständig ist; so zum Beispiel bei telematischen Informationsdiensten, wo die Presseagentur die Informationen sammelt und strukturiert, jedoch ein Informatik- oder Telekommunikationsunternehmen seine Computer nebst interaktiver Software einschaltet und so ihre Abfrage erlaubt;
- die durch die Benutzung einer Dienstleistung angefragten oder entstandenen Daten können an den verschiedensten Orten gespeichert werden; so können sie internationale Netze durchlaufen, oftmals über nicht festgelegte Routen (Veränderungen entstehen aufgrund von Tarifschwankungen, Überbelastungen gewisser Teilabschnitte des Netzes, ...).

1.1 Die verschiedenen Arten von Daten

Hier unterscheiden wir zwischen **a priori entstandenen** Daten, d.h. aufgrund der Zuerkennung einer Karte oder einer Zugangsnummer, die die Benutzung einer Dienstleitung erlauben und **a posteriori entstandenen,** d.h. die durch die Benutzung der Dienstleistung entstehen.

Die Benutzung eines Teleshopping oder Telebankingdienstes erfordert eine vorherige Identifizierung des Benutzers, für die eine Zugangs- oder Geheimnummer (PIN) vonnöten ist; ihre Zuerkennung verlangt jedoch die Angabe gewisser persönlicher Informationen. Dies geschieht im allgemeinen im Rahmen eines Fragebogens, der vor der Unterzeichnung eines Zulassungsvertrags ausgefüllt werden muß.

Die bei der Anfrage einer Zugangsnummer verlangten Informationen beziehen sich auf Beruf, Alter, Namen und Funktion der autorisierten Person. Im allgemeinen sind sie eher banaler Art.

Im Gegensatz dazu geben uns die durch die Benutzung der Dienstleistung entstandenen Daten mehr Anlaß zu Befürchtungen. Hier unterscheiden wir zwischen den Informationen, die **durch die Benutzung der Dienstleistung entstehen** und denen, die im Nachhinein **im Rahmen der Abrechnung der Dienstleistung entstehen.**

Bei den ersteren unterscheiden wir aufs Neue:

- die anläßlich der **Übertragung** entstandenen Daten, eher ungefährlicher Natur, die hinzugefügt werden, um die Umwandlung der Mitteilungen zu ermöglichen;
- die auf die **Verwaltung** bezogenen Daten: Kontonummer, Personal Identification Number (PIN), usw. ...
- die auf den **Inhalt der Mitteilung,** d.h. auf die durchgeführten Operationen, bezogenen Daten.

Diese Informationen betreffen vorwiegend den **Benutzer** (der für ihre Entstehung verantwortlich ist), aber für gewisse Dienstleitstungen auch **dritte Personen** (z.B. den Nutznießer im Rahmen einer elektronischen Zahlung oder Überweisung, vor allem aber bei P.O.S.-Diensten).

Bei den im Rahmen der Durchführung entstandenen handelt es sich vorwiegend um **Rechnungsdaten** (beim Teleshopping) oder um gruppiert ausgewertete Daten, die über den monatlichen Verbrauch von Treibstoffen oder die Verteilung der Transaktionstypen bei den Ausgaben eines Kunden Auskunft geben. Sie betreffen ausschließlich den Benutzer und keine Drittpersonen.

1.2 Die Verarbeitungs- und Speicherungsorte

In der Einleitung dieses Kapitels haben wir auf die Intransparenz der Datenkanäle hingewiesen, über welche die bei einer telematischen Dienstleistung entstandenen Daten fließen.

1.2.1 Die Vielzahl der Orte

Daß diese Behauptung im Rahmen der E.F.T. zutrifft, ist offenkundig: Die durch die Benutzung der Dienstleistung entstandenen Daten werden an mannigfaltigen Orten und durch eine Vielzahl von Personen verarbeitet und weiterversandt, die dem Benutzer meist unbekannt sind. Zu den in den einfacheren Schemen vorkommenden Personen (Zweiparteien-Schemen beim Homebanking oder bei den A.T.M., Dreiparteien-Schemen bei den P.O.S.) müssen noch einige hinzugefügt werden; dies aufgrund von drei Ursachen.

Ein erster Grund ist die **kollektive Organisation** und die hohe Komplexität der Installierung und Verwaltung dieser neuen Zahlungssysteme. Die individuellen Beziehungen zwischen den Kunden und den Banken realisieren sich nur im Rahmen von vertraglichen Beziehungen oder von Vereinigungen zwischen den verschiedenen Partnern (Moschel, Schneider). So schließen sich die Banken im Rahmen der E.F.T. meist in einem Privatnetz zusammen, dessen Verwaltung einem technischen Beauftragten anvertraut wird.

Eine zweite Ursache ist **institutioneller Art**: die europäischen Gesetzgebungen verlangen, daß die Finanzbewegungen innerhalb der Banken eine Kompensierungskammer durchlaufen.

Der dritte Grund ist **technischer Art**: die Datenübertragung läuft über eine Telekommunikationsnetz, das weder Eigentum der Banken noch des technischen Sachverwalters ist. Es gehört in unseren Staaten meist einem öffentlich-rechtlichen Telekommunikationsunternehmen.

Man muß hinzufügen, daß im Falle von P.O.S. die Verarbeitung und Speicherung, sowohl in den einzelnen Filialen, als auch in einem einer Reihe von Unternehmen gemeinsamen Zentrum stattfinden kann.

Diese Einführung zu der Vielzahl von Verarbeitungs- und Speicherorten muß noch durch eine Analyse der durch die Datenübertragung betroffenen oder an den Daten interessierten Personen vervollständigt werden.

1.2.2 Die Interessen der beteiligten Personen

Wir unterscheiden fünf Teilnehmerarten mit verschiedenen Interessen, die teils entgegengesetzt sind, sich aber auch teils ergänzen; zum ersten der **Servicer** (die Bank oder der Herausgeber einer Kreditkarte), sein oder seine technischen Beauftragten sowie der **Benutzer** der Dienstleistung (der Inhaber der Zugangsnummer); sodann, im Rahmen eines P.O.S., der **Kaufmann**, bei dem das Terminal des Telebankingdienstes installiert ist; schließlich der eventuelle **Nutznießer** (Drittperson) einer Telebankingdienstleistung.

Der Vollständigkeit halber müssen wir noch einige Verwaltungen (im Rahmen der Steuergesetzgebung) und die Justiz erwähnen; letztere hat, sowohl bei Streifällen, denen die Benutzung einer Dienstleistung zugrundeliegt, als auch bei strafrechtlichen Verfolgungen ein Interesse daran, Zugang zu den bei der Benutzung einer Dienstleistung entstandenen Information zu erhalten.

A. Die Bank oder der Herausgeber der Kreditkarte

Drei wichtige Interessen befürworten eine Speicherung von personenbezogenen Informationen durch den Anbieter einer Dienstleistung.

- Zum ersten die Notwendigkeit, über eine **möglichst ausführliche analytische Buchführung** jeder telematischen Operationen zu verfügen. Diese analytische Buchhaltung ist vonnöten, um die Abrechnung der Operationen zu sichern (Ausführung einer Zahlungsorder).
- Ein Hinweis auf eine durch einen Benutzer durchgeführte Operation dient, sowohl ihm selbst, als auch den jeweiligen Buchführungsgesetzen gegenüber als **Beweis**. In jedem dieser beiden Fälle hat die Notwendigkeit eines Beweises eine andere Bedeutung: dem Benutzer gegenüber muß der Beweis so vollständig wie nur möglich sein, für die Verwaltung ist dies rechtlich nicht unbedingt vonnöten.
- Schließlich müssen die durch die Benutzung der Telebanking- oder Teleshoppingdienste entstandenen Informationen es dem Servicer erlauben, zu umfangreichen Erkenntnissen über seine Kundschaft zu gelangen. Das bedeutet bei den privaten Kunden, die im Besitz einer Karte sind, Informationen über ihre Verbrauchsgewohnheiten (Typ, Natur, Ort, eventuell sogar den gesamten Inhalt der ausgeführten Operationen), bei den beruflichen Inhabern von P.O.S., Informationen über den Marktanteil bei einem gewissen Kundentyp oder eine Hochrechnung der Verkaufsentwicklung.

Somit verfügt das Finanzinstitut über nützliche Informationen,

- um die Verbreitung seiner eigenen elektronischen Finanzdienstleistungen zu bewerten und dementsprechend seine Marketingpolitik weiterzuentwickeln;
- um eine Marketingpolitik für neue Produkte zu erstellen, da man nun die privaten und beruflichen Kunden besser kennt;
- um die Kreditwürdigkeit eines Kunden zu bestimmen.

B. Der Benutzer der Dienstleistung

Abgesehen von den unbestreitbaren Vorteilen, die ein elektronisches Zahlungssystem im Vergleich zu herkömmlichen Zahlungssystemen bietet, sind auch gewisse Vorteile, die auf einer guten Datenverarbeitung beruhen, nicht von der Hand zu weisen.

Einerseits bietet eine **sofortige Verarbeitung** der Identifizierungsdaten gute Garantien für die **Sicherheit** und die **Fortdauer** der Dienstleistung (so kann der Benutzer, im Falle einer Unterbrechung den Dialog da fortsetzen, wo er ihn begonnen hat). Andererseits hilft die Tatsache, daß er eine Kopie der beim Anbieter gespeicherten Informationen erhält, dem Benutzer bei der **Verwaltung seines privaten Haushaltes**, so daß er jederzeit seinen Ausgaben nachgehen kann; darüberhinaus verfügt er gegenüber dem Kaufmann über einen **Beweis** der durchgeführten Operation, die ihm im Streitfall über die Existenz der Transaktion oder gegenüber gewissen Verwaltungen (zum Beispiel beim Finanzamt: der monatliche Bezinverbrauch) von Nutzen sein kann.

Jedoch stehen **gewisse Befürchtungen** einer Verarbeitung von personenbezogenen Daten entgegen.

Diese Verarbeitung kann seine Freiheit, Kredit zu erhalten, zum Beispiel im Falle einer zu langen Speicherung gewisser Daten (z. B. aufgrund einer mehrmaligen Überschreitung der gedeckten Summe oder aber beim credit scoring, wo Kunden aufgrund gewisser Angaben oder Verbrauchsgewohnheiten ausgeschlossen werden), einschränken; das gleiche gilt für das Recht, Zugang zu einer elektronischen Dienstleistung zu erlangen (aufgrund der Zielgruppeneinteilung der Kundenkreise).

Er kann ebenfalls befürchten, daß eine Verarbeitung die Anonymität gewisser Operationen nicht gewährleistet (zum Beispiel im Falle einer anonymen Schenkung).

Eine Verarbeitung kann auch andere persönliche Freiheiten beeinträchtigen, so zum Beispiel die Meinungsfreiheit (ein Abonnement einer gewissen Zeitung), das Recht, frei innerhalb eines Territoriums zu reisen (Kontrolle der Ortswechsel) usw.

C. Der Kaufmann

Abgesehen von einer garantierten Zahlung mittels einer Kreditkarte, kann man die Einführung von P.O.S. bei einem Kaufmann aus folgenden Gründen rechtfertigen. Zum ersten wird natürlich die Buchführung des Kaufmannes vereinfacht. Darüberhinaus (siehe über die verschiedenen Beweggründe: Priewasser) hat der Kaufmann aus marketingtechnischen Gründen das Bedürfnis, seine Kundschaft genau zu kennen (Verbrauchsgewohnheiten). Schließlich wünscht er bei einem Streitfall, über einen Beweis der Operation zu verfügen; über einen Beweis der besonders unwiderlegbar ist, da er aus den Händen eines Dritten stammt.

D. Die Nutznießer

Verschiedene Gründe lassen den Nutznießer (Dritten) einer elektronischen Überweisung befürchten, daß eine automatische Verarbeitung durch einen Telebankingdienst es gewissen Dienstleistungsunternehmen erlauben könnte, Informationen über ihn zu erhalten (automatische Kontrolle der Einkommensquellen). Eine ähnliche Befürchtung besteht gegenüber anderen teilnehmenden Personen, zum Beispiel dem technischen Beauftragten oder der Bank des Auftraggebers.

E. Der technische Beauftragte

Nur die Speicherung einer Reihe von Informationen durch die Beauftragten ermöglicht eine gute Verwaltung des Netzes; es steht fest, daß der Beauftragte über einen Nachweis der mittels angeschlossener Terminals ausgeführten Operationen verfügen muß. Einerseits um ihre Abrechnung zu garantieren; andererseits um über den aktuellen Kontostand der jeweiligen Inhaber zu verfügen.

Diese Informationen beziehen sich oftmals auf Kunden von verschiedenen Finanzinstituten. Somit verfügt der technische Beauftragte über eine bedeutend vollständigere Übersicht über die verschiedenen privaten und beruflichen Kunden als die einzelnen Mitglieder. Somit wäre es möglich, diese Informationen an einzelne Mitglieder der Vereinigung aber auch an Dritte weiterzureichen.

F. Die Verwaltung (insbesondere die Steuerverwaltung)

Es leuchtet ein, daß die Verwaltung, um die Anwendung der Steuergesetze zu sichern, ein Interesse hat, Zugang zu den verarbeiteten Daten, denen die Benutzung einer telematischen Dienstleistung zu Grunde liegt, zu erhalten. Es geht darum, die Operationen der Kaufleute und Benutzer zu überprüfen.

Aufgrund dieser Tatsache hat das Finanzgesetz von 1984 der Liste der durch Kaufleute anzunehmenden Zahlungsmittel die Zahlungskarten hinzugefügt.

G. Die Richter

Zwei Gründe können einen Einblick in die Datenverarbeitung erfordern: das Vorhandensein einer Operation bei einem Straf- oder Zivilprozeß zu beweisen oder aber die strittige Anwesenheit einer Person an einem bestimmten Ort und zu einem bestimmten Zeitpunkt zu klären.

Diese Darstellung der Besonderheiten, die den E.F.T.-Operationen zugrunde liegt, lenkt unsere Aufmerksamkeit auf die Schwierigkeit, eine gesetzliche Datenschutzregelung in diesem Bereich zu erstellen. Diese muß der Besonderheit der Daten und der Verschiedenheit der beteiligten Personen Rechnung tragen. Schon jetzt scheint uns, daß die Interessen des Benutzers, insbesondere auf dem Gebiet der Sicherheit und des Verbraucherschutzes im Widerspruch zur Erfordernis des Schutzes der Privatsphäre stehen. Somit ist man einer Entscheidung zwischen manchmal widersprüchlichen Zielsetzungen unterworfen.

So kann der Benutzer den Wunsch haben, eine monatliche Aufstellung der an den Terminal durchgeführten Operationen zu erhalten; dann muß er jedoch auch die Verarbeitung und die Speicherung der diesbezüglichen Informationen gestatten.

Die Kreditkartenunternehmen (siehe die von Godschalk zitierten Beispiele) vergrößern die Sicherheit, indem sie Kartendiebstähle anhand von Abweichungen in dem gewöhnlichen Fortbewegungsprofil ihrer Kunden entdecken.

2. Datenschutzregelungen und E.F.T.

Im Gegensatz zu den Schlußfolgerungen einer australischen Arbeitsgruppe, die sich mit den juristischen Problemen des Geldtransfers befaßt, gelangen wir infolge der Überlegungen des ersten Kapitels und der Einleitung zu dem Schluß, daß aufgrund der Besonderheit der Operationen eine spezielle Datenschutzregelung für E.F.T. vonnöten ist.

Seit 1977 faßt die amerikanische National Commission on E.F.T. die Herausforderung durch die Entwicklung der E.F.T. wie folgt zusammen:

- *E.F.T. will create records of financial transactions where were none before;*
- *E.F.T. may increase the amount of information currently included in the financial records;*
- *E.F.T. records in electronically readable form will be easier and less costly to access;*
- *E.F.T. may increase the number of institutions with access to an individual's financial record;*
- *On line, real time E.F.T. systems could be used for surveillance, to locate individuals when they conduct a transaction.*

Um uns dieser Herausforderung zu stellen, schlagen wir vor, die besondere Bedeutung, die die Anwendung der Grundsätze des Übereinkommens des Europarates vom 17. September 1980 haben könnte, zu analysieren. Die Auswahl dieser Referenz hat zwei Gründe. Zum ersten, weil das Parlament, die Kommission und der Ministerrat der Europäischen Gemeinschaften den Mitgliedsstaaten schon mehrmals empfohlen haben, dieses Übereinkommen zu ratifi-

zieren und somit ihre Vorschriften zur Pflicht zu erheben. Zum zweiten, weil dieses Übereinkommen einen gemeinsamen Minimumstandard bildet, der als Grundlage für mehr oder weniger ähnliche Gesetzgebungen in den verschiedenen Mitgliedsländern der Europäischen Gemeinschaft dienen kann.

Die Einführung dieses Standards auf europäischer Ebene, seine Ratifizierung und die Anerkennung gleichwertiger Normen in den Staaten (was noch immer nicht der Fall für Belgien, Italien, Portugal und die Niederlande ist) verfolgen die Absicht, einen gemeinsamen Markt für Telebanking- und Teleshoppingdienstleistungen zu fördern, ohne besondere Befürchtungen um "Privacy" hegen zu müssen.

Die Grundsätze des Übereinkommens des Europarates werden uns als Struktur für den zweiten Abschnitt dieses Kapitels dienen. Jedoch, müssen wir ebenfalls den in bestimmten Ländern bereits bestehenden gesetzlichen Regelungen oder Entscheidungen bezüglich telematischer Dienstleistungen Rechnung tragen.

Der erste Abschnitt befaßt sich mit einigen Prinzipien, die zwar nicht direkt auf die "Privacy"-Regelungen zurückzuführen sind, aber die die "Privacy"-Regelungen ergänzen und somit einen besseren Datenschutz im Rahmen der E.F.T.-Dienstleistungen sichern könnten.

2.1 Die Prinzipien die die Effekte der Datenschutzregelungen verstärken können

Zwei Prinzipien erscheinen uns von Bedeutung:

- das Prinzip des **Bankgeheimnisses**
- das Prinzip des **Briefgeheimnisses.**

2.1.1 Das Prinzip des Bankgeheimnisses

Dieses Prinzip findet sich ebenso in den kontinentalen Rechtssystemen wie in denen des Common Law wieder. Die straf- und verfassungsrechtlichen Gesetzestexte verschiedener Länder bestätigen dies: In Westeuropa geht aus der Jurisprudenz (Tournier v. National Provincial and Union Bank of England 1 K.B. (1924), 461; B.G.H. 4. März 1973; Paris 6. Februar 1975, D., 1975, 318; Cass. b. 25. Oktober 1978, J.T. 1979, 371; Cass it 10. Juli 1974, usw.) eine Verpflichtung des Bankiers zur Diskretion hervor. Diese beinhaltet die vertragliche Haftung gegenüber dem Kunden und eine Haftpflicht gegenüber Dritten; für eine gewisse Rechtslehre sowie einen Teil der Jurizsprudenz geht diese Verpflichtung aus dem Berufsgeheimnis des Bankiers hervor und könnte somit auch strafrechtlich verfolgt werden.

Das Berufsgeheimnis bezieht sich auf vertrauliche Informationen einschließlich der Veränderungen des Kontostandes und anderer durch den Kunden durchgeführter Operationen. Im Gegensatz dazu ist es üblich, einem Kunden mitzuteilen, wenn der Empfänger der Mitteilung über ein legitimes Interesse verfügt, das die Mitteilung dieser Informationen rechtfertigt.

Andererseits steht fest, daß das Bankgeheimnis oder die Verpflichtung zur Diskretion nicht in bezug auf jene Personen besteht, die ein Recht auf diese Mitteilungen haben (im Bereich der E.F.T.: ein anderer Bankier, der durch den Bankier des Kunden beauftragt ist, eine Operation durchzuführen, die der erstere nicht selber durchführen kann; der technische Beauftragte, der mit der Versendung einer elektronischen Nachricht beauftragt ist). In einem elektronischen Zahlungssystem ist es unvermeidlich, daß gewisse dem Bankgeheimnis unterworfene Informationen über von Dritten verwaltete Netze laufen (die technischen Beauftragten). Das Bankgeheimnis kann die Entwicklung dieser neuen Übertragungsmethoden nicht verhindern; einige Autoren fügen hinzu (Schweizer, Mallmann), daß die Verpflichtung zur Geheimhaltung auch auf die technischen Beauftragten ausgeweitet wird.

Schließlich gibt es in allen Festlandstaaten gesetzliche Ausnahmen zur Verpflichtung zur Geheimhaltung:

1. *Der Bankier kann die Zeugenaussage in einem Zivil- oder Strafprozeß nicht unter dem Vorwand des Berufsgeheimnisses verweigern;*
2. *Im Falle einer Inbeschlagnahme des Kontos eines Kunden kann ein Bankier sich nicht hinter seinen Kunden zurückziehen;*
3. *Das gleiche gilt für den Fall, in welchem das Gericht es als nötig erachtet die wirtschaftliche und finanzielle Situation eines Schuldners feststellen zu lassen;*
4. *Das Mitteilungsrecht des Fiskus überwiegt das Bankgeheimnis.*

Der amerikanische **Right to financial privacy Act** von 1978 sieht als Antwort auf die Empfehlungen der Privacy Protection Study Commission Bedingungen für Einzelpersonen und Gesellschaften von weniger als fünf Personen vor. Die Verwaltung erhält die Information entweder aufgrund einer schriftlichen Einverständniserklärung des Kunden oder aufgrund einer formellen schriftlichen Anfrage, einer Mahnung durch Justiz oder Verwaltung oder eines Untersuchungsbefehls. Die gleichen Vorschriftsmaßnahmen wurden bei der Revision des kanadischen Bank Akts von den Banken vorgeschlagen, aber schließlich nicht durch die Regierung übernommen:

„Notwithstanding any provisions of this or any other Act of Parliament or the legislature of a province, documents or records in the possession of a bank relating to the affairs of a customer shall not be subject to inspection or seizure under the authority of any statute or regulation or any order, warrant or other process, and premises of a bank shall not be subject to entry and search for such documents or records, unless there shall have been first delivered to the manager or other person in charge of each branch of the bank from wich such documents or records are sought a written demand specifying the customer of the bank in relation to whose affairs the documents are sought and specifying the documents or records required and unless such written demand shall have been issued by a court of competent jurisdiction or by such other authority as may be empowered by statute to authorize such seizure or search."

2.1.2 Das Prinzip des Briefgeheimnisses

Die Benutzung eines elektronischen Zahlungsdienstes muß als privater Briefwechsel betrachtet werden und somit in den Genuß des Prinzips des Briefgeheimnisses, das durch die Europäische Menschenrechtskonvention garantiert wird, gelangen. Dies ist die Ansicht der Commission française du suivi des expériences télématiques (Französische Kommission für Experimente im Bereich der Telematik), die durch die Definition dieses Begriffs in einem Rundschreiben der französischen Regierung vom 17. Januar 1984 bestätigt wird. Die Tatsache, daß die Übermittlung einer Nachricht auf elektronischem Wege stattfindet, ändert nichts an der Gültigkeit des Prinzips des Briefgeheimnisses.

Diesen französischen Quellen, aber auch den Kommentatoren (Ring-Harstein) des deutschen **Bildschirmtextvertrages** (welcher sich nicht auf private Kommunikationen

bezieht) nach, ist es der Wille des Verfassers einer Nachricht (in unserem Falle des Benutzers eines elektronischen Zahlungsmittels), seine Nachricht geheimzuhalten, der eine private Nachricht definiert; der Überbringer ist lediglich bevollmächtigt, sie der ordnungsgemäß adressierten Person auszuhändigen.

Demzufolge ist es von Bedeutung, daß der elektronische Briefwechsel in den Genuß derselben Geheimhaltungsgarantien gelangt, wie sie dem Postbriefwechsel durch die meisten europäischen Gesetze und Verfassungen zuerkannt werden. Somit werden die Sicherheitsmaßnahmen von allen Personen, sei es der technische Beauftragte der Bank oder ein öffentliches Beförderungsunternehmen, die mit der Übermittlung einer Nachricht betraut sind, anzuwenden sein.

Diesbezüglich ist hinzuzufügen,

1. daß, im Einverständnis mit diesem Prinzip, verschiedene nationale Gesetzgebungen (Großbritannien, Interception of Telecommunications Act, 1985; Portugal, Criminal Code, art. 182), strafrechtliche Verfolgung für jegliches Abfangen von elektronischen Nachrichten vorsehen;
2. daß Artikel 23 der Internationalen Konvention für Telekommunikation von 1983 die nationalen Behörden, die sich mit der Telekommunikation befassen, verpflichtet, Maßnahmen zur Sicherung der Einrichtungen und Netze zu ergreifen.

Schlußfolgerung des ersten Abschnittes

Die Prinzipien des Brief- und des Bankgeheimnisses müssen auf dem Gebiet der elektronischen Nachrichtenübermittlungsdienste gelten.

Das Prinzip des Bankgeheimnisses verstärkt die Verpflichtung der Nicht-Mitteilung von personenbezogenen Informationen durch den Bankier, einerseits gegenüber Personen, die nicht dem Bankwesen angehören, so den Kaufleuten, den Inhabern von P.O.S., andererseits auch gegenüber Personen, die am Erwerb von Wirtschaftsinformationen interessiert sind (Informationsagenturen, Adressenherausgeber, ...).

Das Prinzip des Briefgeheimnisses bestätigt die Respektierung der Vertraulichkeit von elektronischen Botschaften, gleichermaßen wie es den Beförderern vorschreibt, technische Maßnahmen, die eine größere Sicherheit der Nachrichten gewährleisten, zu treffen.

2.2 Die Anwendung der Grundsätze der Datenschutzregelungen auf E.F.T.

In der Einleitung zum zweiten Kapitel haben wir die Wahl des Übereinkommens des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten als Ausgangspunkt für unsere Überlegungen bezüglich der speziellen, im E.F.T. zutreffenden Maßnahmen gerechtfertigt. Aus dem ersten Kapitel ging hervor, daß die Besonderheit der Durchführung von E.F.T.-Operationen zusätzliche Präzisierungen, Anpassungen und Vervollständigungen der bestehenden Regelungen erfordert.

Verschiedene Gesetzgebungen oder nationale Entscheidungen haben dem schon Rechnung getragen; dementsprechend werden sie bei der Erörterung der Grundsätze des Europarats erwähnt.

Somit folgen wir der Struktur des Übereinkommens:

I. Grundsätze bezüglich der Begriffsbestimmungen und des Geltungsbereichs des Übereinkommens (Artikel 2 der Konvention);

II. Grundsätze bezüglich der Einführung und Durchführung der Operationen (Artikel 5–7 der Konvention);

III. Grundsätze bezüglich des Zugangsrechtes der registrierten Person (Artikel 8 der Konvention);

IV. Grundsätze bezüglich des grenzüberschreitenden Verkehrs der Datenströme, die durch diese Operationen entstehen (Artikel 12 der Konvention).

2.2.1 Definitionen und Anwendungsbereich

Drei Begriffsbestimmungen sind von Bedeutung:

- **personenbezogene Daten**
- **automatische Datei**
- **Verantwortlicher für eine Datei**
  (diesem Ausdruck entspricht in der Bundesrepublik Deutschland der Begriff „speichernde Stelle").

Der Begriff der personenbezogenen Daten bezieht sich auf jede Information über eine natürliche Person. Man weiß von der allgemeinen Zurückhaltung der Datenschutzregelungen, (außer Österreich, Luxemburg, Norwegen, Dänemark, ...) ihren Schutz auf juristische Personen auszudehnen. Das in einem kürzlich erschienenen Bericht der O.T.A. analysierte amerikanische „E.F.T. Privacy Act"-Projekt erweitert seinen Schutz auf die kleineren und mittleren Unternehmen. Dies begründet man damit, daß eine diesen Unternehmen ausgehändigte Karte, aufgrund der personenbezogenen Verwaltung in Betrieben dieser Größenordnung, ebenfalls personenbezogene Daten entstehen läßt.

Der Begriff der automatisierten Datei, so wie er aus dem Übereinkommen und den meisten nationalen Gestzgebungen hervorgeht, legt das Vorhandensein einer zentralen Verarbeitung, die einfach zu lokalisieren ist, nahe. Auf dem Gebiet des E.F.T. bildet eine Datensammlung jedoch nicht eine Einheit, sondern verteilt sich über eine Vielzahl von Orten: lokale Dateien in den P.O.S. oder A.T.M., die auf lokaler Ebene funktionieren, Netze mit Speicher, regionale Informatikzentren der Banken usw.

In dem Maß, in dem der Begriff Datei an Bedeutung gewinnt, um den registrierten Personen Zugang zu ihren Daten zu ermöglichen, erscheint es vonnöten, zu überprüfen, wie man das Vorhandensein einer „logischen Datei" nachweisen kann, um dann schließlich die Wiedergewinnung aller, aufgrund einer legitimen Verarbeitung und Speicherung im Netz verstreuten Daten vorzunehmen (Europarat).

In diesem Sinne, und um den Einfluß des Netzes auf die Verarbeitung der bei der Benutzung eines elektronischen Zahlungsdienstes benötigten oder entstandenen Informationen zu verdeutlichen, ist es von Bedeutung, den Begriff Verantwortlicher für die Datei zu zu definieren als **„Verantwortlicher für das Netz"**, das heißt, der Person, die für die Gesamtheit der personenbezogenen Daten in einem Netz oder noch besser für eine **logische Datei** (im Gegensatz zur physischen Datei, wie aus den Arbeiten des Europarats bezüglich der Bedeutung der Telemetrie, der interaktiven Medien und der elektronischen Nachrichtensysteme hervorgeht) verantwortlich ist.

Die Idee eines in bezug auf die registrierten Personen **einzigen Verantwortlichen** für die Gesamtheit der Verarbeitungen (die auf der Ein- und Durchführung von elektronischen Zahlungsdienstleistungen beruhen) und deren

Konformität zur Datenschutzregelung steht im Einklang mit den Vorstellungen der Rechtslehre und der internationalen Organisationen (UNCITRAL) bezüglich der zivilrechtlichen Haftung im Falle einer irrtümlichen oder betrügerischen Mißachtung der Zahlungsinstruktionen. Sie versteht sich im Sinne einer Vereinfachung der Rechtsmittel für den Benutzer elektronischer Zahlungsmittel und bezeichnet ganz einfach den Bankier oder den Herausgeber eines elektronischen Zahlungsmittels als verantwortlich für die Gesamtheit des Netzes.

2.2.2 Grundsätze bezüglich der Einführung und Durchführung von E.F.T.

In den Artikeln 5–8 des Übereinkommens des Europarates finden wir eine Reihe von Grundsätzen, die wir nur zum Teil analysieren, d. h. in dem Maße, in dem sie den E.F.T. angepaßt werden müssen. So ist der Grundsatz der Qualität der Daten (sachlich richtig, auf dem neuesten Stand) auf die E.F.T. genauso wie auf alle anderen Arten von Datenverarbeitungen anwendbar. Unsere Erörterung beschränkt sich somit **ausschließlich auf die Grundsätze der Beschaffung auf rechtmäßige Weise, der Sicherheit und schließlich auf den wichtigsten, den Grundsatz der Zweckmäßigkeit.**

A. Der Grundsatz der Beschaffung nach Treu und Glauben und auf rechtmäßige Weise

Im ersten Kapitel haben wir festgestellt, daß vorwiegend die durch die Benutzung der Dienstleistung entstandenen Daten betroffen sind. Dies unterstreicht die Wichtigkeit, dem Benutzer solcher Dienstleistungen sowohl die Tatsache der Registrierung dieser personenbezogenen Daten, als auch deren Zweck ins Bewußtsein zu rufen. Hieraus gehen einerseits die Idee der **Transparenz** der Informationsströme und deren Inhalte, sowie andererseits die Idee des **freien und bewußten Einverständnisses** der registrierten Person mit solchen Verarbeitungen hervor.

Wenn wir vom Grundsatz des Zugangsrechtes sprechen (infra 2.2.3), haben wir Gelegenheit, auf die Informationspflicht zu Lasten des „Verantwortlichen für das Netz" zurückzukommen. An dieser Stelle erklärt ein Auszug aus einem Bericht der O.T.A. noch einmal die Bedeutung der gerade erwähnten Ideen:

"in payment systems, privacy is violated when data are, without the subject's consent, made available to and used by those not a party to the transaction, for purposes other than those necessary to accomplish the transaction. Those other purposes could range from organized market campaigns to Goverment Surveillance to blackmail. If a person has neither explicity nor implicity consented to disclosure and use of information for a given purpose, personal privacy is considered to have been violated even if the same information was willingly provided by that person, either to another party or to the same party for a different purpose".

B. Der Grundsatz der Sicherheit

Aus der Besonderheit der bei telematischen Finanzdiensten vorgenommenen Verarbeitungen geht die Vielfalt der Verarbeitungsorte deutlich hervor, insofern ist es absolut unmöglich, ein System physikalischer Sicherheit vorauszuplanen (zum Beispiel: A.T.M. an öffentlichen Plätzen).

Die Verpflichtung, **„geeignete Sicherheitsmaßnahmen"** zu treffen, zwingt uns, die Gesamtheit des oder der Übertragungsnetze einschließlich der Zugangskarte in Betracht zu ziehen. Insbesondere wenn es sich um Chipkarten handelt, ist der Anbieter der Dienstleistung verpflichtet, alle Maßnahmen zu treffen, es nur den zugelassenen Personen zu ermöglichen,Zugang zu den gespeicherten Informationen zu erhalten (C.N.I.L., 5. Aktivitätsbericht, 1985, p. 150). Bezüglich der Datenübertragung ist es für gewisse Operationen von Interesse, zur Anwendung von Sicherheitsschlüsseln (Chiffriermethoden) zu verpflichten.

Angesichts der Tatsache, daß auf diesem Gebiet ein öffentliches Interesse von Bedeutung mitspielt, ist eine direkte oder indirekte gesetzliche Regelung zu empfehlen (Genehmigung, Lizenz). Letztere Lösung, bedeutend elastischer handzuhaben und außerdem der technischen Entwicklung Rechnung tragend, könnte in ein Projekt zur Überprüfung der Dienstleistungszentren eingegliedert werden (siehe den Bericht Monville-Poullet im Rahmen von FAST: Die Endnachfrage in der Telematik – juristische Aspekte). Die Überprüfung dieser Dienstleistungszentren (insbesondere der technischen Beauftragten) vollzieht sich auf der Grundlage eines Sicherheitsplans, der durch die mit der Normierung beauftragten Instanzen sowie durch die Datenschutzbehörden festgelegt wird.

C. Der Grundsatz der Zweckmäßigkeit

Die Anwendung dieses Grundsatzes auf die im Rahmen von E.F.T. durch die verschiedenen Teilnehmer vorgenommenen Verarbeitungen war Anlaß zu einer Vielzahl von Überlegungen und Anpassungen. Für Baumann, Bundesdatenschutzbeauftragter (Goldschalk), hat dieser Grundsatz drei Bedeutungen:

- So wenig Datenspeicherung wie möglich;
- Die Speicherung der für das Bankgeschäft notwendigen Daten soll zeitlich begrenzt werden.
- Die Datenflüsse sollen so organisiert werden, daß die Transparenz für den Betroffenen maximiert und die Mißbrauchsmöglichkeiten minimiert werden.

Zwei dieser Überlegungen gehören zu den Pflichten und Rechten der Person, die wir als den „Verantwortlichen des Netzes" bezeichnet haben, die dritte beinhaltet die Anwendung des Grundsatzes auf die Datenübertragungen und -verarbeitungen, die durch die anderen von der Durchführung von E.F.T.-Operationen betroffenen Personen vorgenommen werden. Wir analysieren beide getrennt.

1) Der Grundsatz der Zweckmäßigkeit und seine Anwendung auf den Verantwortlichen des Netzes

Die Anwendung dieses Grundsatzes auf die durch den Verantwortlichen der Datei vorgenommenen Verarbeitungen zieht vorwiegend dreierlei Folgen nach sich:

- zum ersten bezüglich des **Inhaltes der Verarbeitung;**
- zum zweiten bezüglich der **Dauer der Speicherung;**
- zum dritten bezüglich der **Art der Verarbeitung.**

a) Der Inhalt der Verarbeitung

Der Artikel 24 (1) des dänischen Gesetzes über Zahlungskarten sieht vor:

"24-(1) Only information on card holders necessary for the carrying out of payment transaction and information on instances where a payment card has disappeared or been revoked due to misuse may be registered."

In diesem Artikel finden wir den Grundsatz der Erheblichkeit, der in der deutschen, dänischen und österreichischen Gesetzgebung vorkommt, wieder; ihmzufolge dürfen nur die erheblichen, d. h. die zur Durchführung der Operationen unbedingt notwendigen Daten, die in dem mit dem Betroffenen geschlossenen Vertrag vorkommen, registriert werden.

Eine Empfehlung der N.C.E.F.T. vervollständigt diesen Grundsatz auf geschickte Weise:

"Government should minimize the extent to wich it requires an institution to maintain and report records about an individual using an E.F.T. system, and should minimize the extent to wich it requires information to be collected that is not necessary to the operation of the E.F.T. system."

b) Die Dauer

Artikel 25 des bereits zitierten dänischen Gesetzes enthält eine Vorschrift bezüglich der Dauer, die sowohl die Aufmerksamkeit der N.C.E.F.T. als auch der Schweizer Bundeskommission für Verbrauch und des Französischen Nationalrates für das Kreditwesen erregt hat.

"25 Information on the use of payment systems by individuals and bussinessers is filed for five years whereupon it is destroyed. However, information on misuse shall be destroyed two years after the registration at the latest."

Es bleibt noch zu bemerken, daß andere Quellen die Löschung der Informationen bei Ablauf des mit dem Betroffenen geschlossenen Vertrages fordern.

c) Die Arten der Verarbeitung

Die Empfehlung der N.C.E.F.T. ist bemerkenswert:

"E.F.T. systems should not be used for surveillance of individuals as to their location or patterns of behaviour."

Diesbezüglich erinnern wir daran, daß die französische Gesetzgebung (hierbei der CNIL und dem Bericht des Französischen Nationalrates für das Kreditwesen folgend) untersagt, eine Entscheidung, die die **Bewertung eines menschlichen Verhaltens**, beinhaltet, ausschließlich auf der Grundlage „einer automatischen Datenverarbeitung, die das Vermögen oder die Persönlichkeit des Betroffenen beinhaltet" zu treffen. Dies betrifft sowohl die Kreditinstitute als auch die Kaufleute, die die anläßlich der Benutzung einer Dienstleistung entstandenen Daten zur **Auswahl ihres Kundenkreises** nutzen (zu dieser Überlegung kam auch die Schweizer Bundeskommission für Verbrauch).

Die gleichen Überlegungen verbieten auch jede Abtretung (ohne das Einverständnis der registrierten Person) von Informationen an Dritte. Über die Verwendung für Mailingdienste muß der Kunde schriftlich informiert werden. Diese verschiedenen Vorschriften schränken das Recht der Datenverwendung durch den Verantwortlichen des Netzes ein und zwingen ihn, dem Grundsatz der Transparenz dieser Verwendungen, der auch im Bildschirmtextvertrag übernommen wurde, zu folgen. Artikel 9 des Bildschirmtextvertrages sieht vor, daß im Bereich der telematischen Dienstleistungen, die genehmigten Verwendungszwecke durch eine gesetzliche Regelung **a priori** festgelegt werden müssen. Dies steht im Gegensatz zu den meisten anderen Verarbeitungen, wo es, dem Prinzip der Erheblichkeit folgend, dem Unternehmen selbst obliegt, die für seine Funktionsfähigkeit notwendigen Verwendungen festzulegen, in diesem Falle jedoch unter der Einschränkung einer **a posteriori** stattfindenden Kontrolle durch die Gerichte oder eine andere Behörde (Poullet).

Artikel 9 des Bildschirmtextstaatsvertrages, der auch auf die Teleshopping- und Telebankingdienstleistungen angewandt wird, schränkt von vornherein die Verwendungen und die Speicherungsdauer personenbezogener Daten ein.

Artikel 9 Absatz 3 des Staatsvertrages schreibt vor, daß die Bundespost (gleichzeitig Inhaber und Dienstleister) ausschließlich die Daten, die zur Erstellung der Rechnung für die Mitteilungen notwendig sind, verarbeiten darf; d. h. ohne daß Dauer, Art, Inhalt und Betrag der Operation erkennbar sind. Er präzisiert, was man unter den für die Rechnungserstellung notwendigen Daten versteht, daß außerdem die Abtretung sowie die Erstellung eines Verbraucherprofils durch die Bundespost untersagt sind und daß die Speicherungsdauer auf die für die Eintreibung notwendige Dauer beschränkt ist.

Absatz 6 § 2 des gleichen Artikels verbietet außerdem dem Betreiber des Dienstes, die Bekanntgabe oder die Erstellung eines Profils, es sei denn, mit Einverständnis des Benutzers. Die Unternehmen, die mit der Ausführung der Dienstleistung betraut sind, unterliegen der gleichen Pflicht (Ring, Hartstein).

In diesem Sinne möchten wir Artikel 24 (2) und (3) des dänischen Gesetzes zitieren:

(2) "Information on card holders may only be used and disclosed when necessary for carrying out of payment transactions, corrections and legal enforcement, or when authorised by legislation. Information on misuse may only be disclosed to the extent necessary to avoid further misuse."

(3) "Information on payment creditors may only be used and disclosed when necessary for carrying out of payment transactions, corrections and legal enforcement, or when authorised by legislation. Information may otherwise only be disclosed to the extent authorised by other legislation."

Schlußfolgerung

Das Prinzip der Erheblichkeit, das in der Übereinkunft des Europarates (Artikel 5) und in einigen nationalen Gesetzgebungen (insbesondere BRD und Dänemark) erwähnt wird, verpflichtet den Betreiber eines Telebankingdienstes deutlich, die gesetzmäßigen Zielsetzungen seiner Verarbeitung, die Art der für die Durchführung der Operationen benötigten Daten und deren Speicherungsdauer zu präzisieren. (Was geschieht zum Beispiel im Falle einer Speicherung über das Bestehen des Kontos hinaus; Französischer Rat für Kreditwesen, Bericht über die juristischen Gesichtspunkte der neuen Zahlungsmittel, Juli 1986).

Eine flexible und evolutive Annäherung, wie sie dieser Grundsatz erlaubt, ist von Vorteil, sei es, um eine den verschiedenen Datenarten angepaßte Regelung über Datenbanken zu erstellen, oder auch um eine vorherige Erlaubnis des Betroffenen oder einer Datenschutzbehörde zu erhalten. Der Grundsatz der Erheblichkeit erlaubt eine flexible Anpassung an den betroffenen Sektor; somit sind die jeweiligen Verbände verpflichtet, die Zielsetzungen ihrer Verarbeitung von personenbezogenen Daten festzulegen.

Die Registrierung von personenbezogenen Daten, die durch die Benutzung der Dienstleistung entstehen, haben beim Telebanking folgende legitime Zielsetzungen:

1. die Ausführung von Zahlungsordern;
2. die Notwendigkeit der Datenspeicherung für den Fall von Beschwerden der Benutzer;
3. die Möglichkeit, Marktanalysen vorzunehmen.

2) Andere von der Durchführung der Operationen betroffene Personen

Ein kürzlich erschienener Bericht über das amerikanische "E.F.T.-Privacy Act"-Projekt führt den Begriff der "E.F.T.-Service-Provider" ein:

"Any person who provides services including data processing telecommunications and courier services, intended to acomplish or to facilitate, during the period between

initiation and completion of a transfer, en electronic fund transfer, but only in regard to the operations of the person in the actual provision of services intended to acomplish or facilitate an electronic fund transfer."

Dieser Begriff erstreckt sich somit auf alle an den Operationen beteiligten Personen einschließlich des Kaufmanns, bei dem das Terminal installiert ist. Er schließt jede Person, mit Ausnahme des Verantwortlichen für das Netz, die persönlich an der Ausführung einer elektronischen Transfers beteiligt ist, ein.

Die anderen beteiligten Personen sind einerseits der **Kaufmann, der Inhaber des P.O.S. ist,** andererseits **die verschiedenen am Banksystem beteiligten Personen, deren Einbeziehung durch die jeweilige assoziative (der technische Beauftragte) oder geregelte Struktur gerechtfertigt ist.**

Bezüglich der letzteren unterscheidet man in Deutschland, Österreich und Dänemark zwischen Unternehmen, die **im Rahmen ihrer eigenen Aktivitäten arbeiten**, und Unternehmen, die **im Auftrag eines anderen** intervenieren. Dies gestattet, die mit der technischen Durchführung betrauten Dienste, die Kompensierungskammern und die Transporteure einer strengeren Gesetzgebung zu unterwerfen (keine dieser Personen ist am Operationsvertrag beteiligt).

In der deutschen Rechtsprechung bezüglich der Schufa, eines von den Banken gegründeten Informationszentrums, das ausschließlich den Mitgliedsbanken Auskünfte über den Kontostand der Kunden dieser Banken gibt, finden wir einige interessante Grundsätze. Sie begrenzen Aktivitäten der technischen und institutionellen Beauftragten, die für Dritte Daten speichern. Die Bekanntgabe von personenbezogenen Informationen an die Schufa ist nur mit Einverständnis des Betroffenen gestattet. Mit anderen Worten, die Bildung eines Auskunftspools durch die Banken setzt das Einverständnis der zu registrierenden Personen voraus. Erlaubt hingegen ist die Bekanntgabe von Informationen durch die Schufa, jedoch nur in dem Maße, wie ihre Bekanntgabe, ihre zeitlich begrenzte Speicherung und ihr Inhalt vonnöten sind, um die vertraglich mit dem Betroffenen vereinbarten Dienstleistungen zu ermöglichen. Es bleibt noch hinzuzufügen, daß die Schufa diese Informationen auf keinen Fall kommerziell verwenden darf (Mallmann, Moschel).

In diesem Sinne verstehen sich auch die vereinfachten Normen Nr. 12 und 13 des französischen CNIL über die Verwaltung von Bankkonten und Kreditverträgen. Wir müssen jedoch hinzufügen, daß das CNIL (Protokolle Nr. 14 und 15) die ursprüngliche Version des Nicht-Mitteilungsprinzips übernimmt, somit mußte es die innerhalb der Banken stattfindende Verteilung von Schwarzen Listen (bei Verlust, Diebstahl und Überschreitung des gedeckten Betrages) erlauben, bestand jedoch darauf, die Verbreitung dieser Informationen und vor allem ihre Aufbewahrungszeit im Auge zu behalten.

In den Vereinigten Staaten schließlich (siehe Brown) gilt das Prinzip der Einschränkung der Verbreitung von Informationen selbst gegenüber den technischen Beauftragten. Die Empfehlungen des N.C.E.F.T. sehen vor:

"There should be no disclosure to private sector without specific authorization by the subject, and certification by the recipient that data will be used only for the designated purpose;

Information may be given to support organizations performing routine services for the financial institution, provided it certifies that it will maintain confidentiality;

Information may be disclosed to participants and intermediaries to a transaction; intermediaries include "authorizing/guaranteening organizations";

Information related to fraud and other crime can be disclosed to law inforcement officers, and customer delinquency can be disclosed to other E.F.T. offerings institutions, credit granting organizations, ...;

Kaufleute, die über P.O.S. verfügen, können ebenfalls Interesse daran haben, über die Bank in den Besitz gewisser Kundendaten zu gelangen. Abgesehen vom Grundsatz des Bankgeheimnisses sind der Bank auch andere, spezifischere Einschränkungen ihres Mitteilungsrechts gegenüber Kaufleuten gesetzt. Schneider meint, daß der Kaufmann weder Zugang zu den Schwarzen Listen noch zum Kontostand haben darf; CNIL folgend erklärt der Französische Rat für Kreditwesen, daß ein Kaufmann, der die durch ein P.O.S. gesammelten personenbezogenen Daten dazu verwendet, seine Kunden zu selektieren, dem Gesetz über Informatik und Grundrechte und einer Meldepflicht am CNIL unterworfen ist; darüberhinaus erinnert er daran, daß es untersagt ist, eine Entscheidung zu fällen, die ausschließlich auf „einer automatischen Datenverarbeitung zum Zwecke, ein Profil oder die Persönlichkeit des Betroffenen festzustellen", beruht (Art. 2 des franz. Gesetzes).

2.2.3 Das Zugangsrecht der registrierten Person

Unter diesem Zugangsrecht versteht man jede Maßnahme, die es jemandem ermöglicht, eine angemessene Transparenz der Informationen und Datenströme im Rahmen der E.F.T. zu erlangen.

Diesbezüglich ist Artikel 13 des dänischen Gesetzes von 1984 über Zahlungskarten von Interesse. Er erwähnt die Informationen, insbesondere personenbezogene Daten, die vor der Auslieferung einer Zahlungskarte schriftlich angegeben werden müssen; die Verwendung, Verarbeitung und Mitteilung von personenbezogenen Daten und die durchgeführten Operationen; die Maßnahmen, die dem Mißbrauch von verlorengegangenen oder in den Besitz nicht autorisierter Personen gelangter Karten vorbeugen sollen.

Desgleichen sieht der E.F.T.-Act von 1978 schon vor, daß der Kunde bei der Unterzeichnung eines Vertrags für die Benutzung von E.F.T.S. über die jeweilige Politik des Finanzinstitutes bezüglich der Bekanntgabe der personenbezogenen Daten (die durch die Benutzung oder die Verarbeitung des Systems entstehen) informiert wird. Eine Empfehlung des N.C.E.F.T. sieht vor, daß „der Kunde Zugang zu allen gespeicherten Daten hat und ihren Inhalt widerrufen kann".

Verschiedene Autoren (Godschalk, Schneider, sich auf eine Empfehlung der Schweizer Bundeskommission für Verbrauch berufend) schließen aus dem Grundsatz der Transparenz, daß die auf der Karte sowie die auf andere Weise mitgeteilten Informationen genau mit den gespeicherten Daten übereinstimmen. Es sei ausgeschlossen, der Karte verschlüsselte Geheiminformationen, die dem Kunden unbekannt sind, hinzuzufügen (diesbezüglich § 905 des amerikanischen E.F.T.-Act). Diese Überlegungen betreffen insbesondere die Chipkarten.

2.2.4 Internationale Gesichtspunkte von E.F.T. und Datenschutz

Aus Artikel 12 des Übereinkommens geht der Grundsatz des Verbots jeglicher Einschränkung des grenzüberschreitenden Verkehrs hervor. Mit der Ratifizierung des Übereinkommens finden wir auch in den nationalen Gesetzge-

bungen „gleichwertige" Regelungen. Die Empfehlungen der O.E.C.D. folgen dem gleichen Prinzip.

Man muß anerkennen, daß einige neuere Gesetzgebungen die Finanzinstitute, die E.F.T.-Dienstleistungen anbieten, verpflichten, ihre für die Ausführung der Dienstleistung notwendige Verarbeitung ausschließlich innerhalb der Landesgrenzen durchführen. So verfügt Artikel 26 des dänischen Gesetzes über Zahlungskarten:

"Having obtained the opinion of the Data Surveillance Board (die mit der Kontrolle des Datenschutzes betraute Organisation), the Ministry of Industry shall make regulations directing that information relative to persons domiciled in the country may only be registered and processed in this country."

Der kanadische Bank Act von 1980 verpflichtet die Banken ebenfalls, die Daten ihrer in Kanada wohnenden Kunden innerhalb der Landesgrenzen zu verarbeiten.

Diese beiden Vorschriften stehen in engem Bezug zu der im Bildschirmtextvertrag erwähnten Verpflichtung, daß die Unternehmen die innerhalb der Landesgrenzen telematische Dienstleistungen anbieten, verpflichtet sind, eine Agentur zu gründen, die den deutschen Datenschutzbehörden gegenüber verantwortlich ist (Ring-Harstein). Artikel 45 des österreichischen Bildschirmtextprojektes sieht eine Verpflichtung der ausländischen Anbieter vor, sich den österreichischen Datenschutzbestimmungen zu unterwerfen.

Diese Referenzen klären uns über die besonderen Gefahren, die mit den telematischen Dienstleistungen und insbesondere E.F.T. auftreten, auf. Es bleibt uns, die Notwendigkeit zu unterstreichen, daß internationale Standards geschaffen werden, die „nationalen Reflexen" zuvorkommen; wie zum Beispiel die Verpflichtung der Unternehmen, ihre Daten ausschließlich innerhalb der Landesgrenzen zu verarbeiten, die zur Folge hat, daß sie ihre Dienstleistungen nicht im Ausland anbieten können. Im Gegensatz hierzu steht fest, daß für eine Weiterentwicklung der E.F.T. die Einrichtung von europäischen ja Weltnetzen vonnöten ist.

Schlußfolgerungen

Aus dieser kurzen Erörterung der Regelungen gehen folgende Grundsätze hervor:

- Die Notwendigkeit, die erheblichen Verwendungen der personenbezogenen Daten, die durch die Benutzung dieser Dienstleistungen entstehen, die Aufbewahrungsdauer dieser Daten, sowie das Verbot gewisser Verwendungen (Dateien an Dritte weiterzureichen) im voraus festzulegen (siehe Artikel 9 des Btx-Staatsvertrages, sowie die dänische Gesetzgebung);
- Die Anerkennung eines erweiterten Informationsrechtes für den Verbraucher von Telebanking- und Teleshoppingdienstleistungen, insbesondere bei der Anforderung einer Karte oder ab der ersten Benutzung einer Dienstleistung;
- Die Anerkennung eines besonderen Status für Drittunternehmen, die somit den selben Berufspflichten wie dem Servicer unterliegen (siehe das amerikanische Projekt "E.F.T.-Privacy Act" sowie die Erörterungen über die Normen der CNIL).

Stichwörter: Informativer Wert elektronischer Zahlungen – besondere Gefahren der E.F.T. – Operationen – verschiedene Arten von Daten – Vielzahl von Verarbeitungs- und Speicherungsorten – Mannigfaltigkeit der Interessen der beteiligten Personen – Prinzipien, die den Effekt der Privacy Regelungen verstärken können – Bankgeheimnis, Briefgeheimnis – Grundsätze des Europarates – Begriffsbestimmung, Geltungsbereich, Durchführung der Operationen, Erheblichkeit, Zugangsrecht der registrierten Person – grenzüberschreitender Verkehr – die Verwendung der Daten im voraus definieren – Informationsrecht des Verbrauchers – besonderer Status für alle an der Durchführung beteiligten Personen.

Literatur

Ellis, M. B., Greguras, M.: The E.F.T. Act. Prentice Hall ed., New York, 1983.

Conseil National du Credit: Rapport juridique sur les aspects juridiques des nouveaux moyens de paiement, Juli 1986.

Craddock, C.: Privacy and Equity in E.F.T.S.: Some basic issues. *The Canadian Banker and ICB Review.*

Zaki, A.: Regulation of E.F.T. Impact and Legal Issues, *Comm. of the ACM.* Feb. 1983.

Schneider, J.: Datenschutz und Neue Medien, *NJW* 1984, 390.

Borsum, W., Hoffmeister, V.: Bildschirmtext und Bankgeschäfte, doc. polycopié, Institut für Recht und Informatik, Hannover 1984.

Lambert, J.: E.F.T. Systems. The Emerging Legal Issues. *The Law Society's Gazette.* 14. Nov. 1984.

Dauer, E.: The Policy implications of neutral Scholarship; a Case Study of E.F.T. and the Baxter, Cootner and Scott Report, 2. *Cardozo L. Rev.*, 1981, 397 et s.

Delahaie, H., Grissonanche, A.: Les nouveaux de paiement, *Cahiers de droit*, 1983, 301 et s.

Zimmer, R. C., Einhorn, Th.: The Law of E.F.T., Washington D.C., Card Services, Inc., 1978, 23–31.

Marchand, D. A.: Privacy. Confidentiality and Computers. National and International Implications of U.S. Infromation Policy, *Telecommunications Policy*, Sept. 1979.

Godschalk, H.: Datenschutz am Point of Sale, *Computer und Recht*, 1987, n° 7, 416 et s.

Heller, C. E.: Privacy and the public good, in Computers and Banking, E.F.T. Systems and public Policy, K. W. Colton and K. L. Kraemer (ed.), New York, 1980, 92 et s.

O.T.A.: Selected Electronic Funds Transfer Issues: Privacy Security and Equity, Background Paper, Congressional Board of the 94th Congress, 1982.

Tigert, R. R.: Legal Aspects of E.F.T. in the U.S., *Intern. Bankung Law*, Feb. 1984, 101 et s.

Brown, J. L.: Implications of the informational nature of payments, *Computer Law Journal*, 1980, 2, 153 et s.

Poullet, Y.: Privacy et services electroniques d'information, in Electronic information Services; Legal Aspects, Report prepared for the Legal Observatory of the european Commission, Jan. 1987.

Mallmann, O.: Datenspeicherung und -übermittlung, in Komm. zum B.D.S.G., 3° ed., Baden-Baden, Nomos, 1981.

Schweizer, R.: La protection des données et autres problèmes juridiques des nouveaux moyens electroniques de paiement, in Les nouveaux moyens électroniques de paiement, B. Stauder (ed.), Coll. jurid. romande, Payout, Lausanne, 1986.

Kaiser, T.: Legal implications of automated teller Machines, London School of Economics, Juni, 1985.

Parker, D.: E.F.T. and National Security, *Information Age*, 1982, 19 et s.

Dux, C.: Credit Clearing. Stellen und Datenschutz. *Datenschutz und Datensicherung*, 1985, 147 et s.

Dammann, U., Stange, H. J.: Reform des Datenschutzes im Kreditinformationssystem, *Zeitschrift für Wirtschaftsrecht*, 1986, 486 et s.

Westin, A.: Privacy Issues and the implications of in Home Banking, *American Banker*, Juni 3, 1981.

Moschel, W.: Dogmatische Strukturen des bargeldlosen Zahlungsverkehrs, *AcP*, 1986, 187 et s.

Les nouveaux moyens de paiement: Droit, Argent et libertés, Actes du 17° congrès national des huissiers de justice, Dijon, septembre 1986, J.-P. Farget (ed.), Economica, Paris, 1986.

Froystad, D.: Data protection in practice: identifying and matching elements, Teresa (17), Complex, N.R.C.C.L., Oslo, 1984.